

سند شرح نیازمندی‌های توسعه وب‌اپلیکیشن کنترل پنل دزدگیر سیم‌کارتی از طریق پیامک (SMS)

عنوان پروژه: طراحی وب‌اپلیکیشن مدیریت و کنترل دزدگیر سیم‌کارتی

نوع پروژه: Web Application / PWA

روش ارتباط با دستگاه: پیامک (SMS) از طریق سیم‌کارت نصب‌شده روی تلفن همراه کاربر

۱. معرفی پروژه

هدف پروژه، طراحی و توسعه یک وب‌اپلیکیشن فارسی برای کنترل و مدیریت دزدگیرهای سیم‌کارتی است. کاربر باید بتواند بدون نیاز به تماس تلفنی با دستگاه یا ارسال دستی پیامک، از طریق یک رابط کاربری ساده، فرمان‌های موردنیاز را برای دستگاه ارسال کرده و وضعیت دستگاه و گزارش رویدادها را مشاهده کند.

این سامانه باید با دزدگیرهای سیم‌کارتی موجود که از طریق پیامک کنترل می‌شوند سازگار باشد و امکان توسعه آن برای مدل‌های مختلف دستگاه در آینده وجود داشته باشد.

نکته مهم: ارتباط اصلی این نسخه از طریق SMS است؛ بنابراین دستگاه برای دریافت فرمان‌ها نیازی به اینترنت یا اتصال مستقیم به سرور ندارد. ارسال فرمان از طریق وب‌اپلیکیشن و سرویس پیامکی انجام می‌شود.

۲. اهداف اصلی پروژه

- کنترل وضعیت دزدگیر از طریق وب‌اپلیکیشن.
- ارسال خودکار پیامک‌های فرمان به شماره سیم‌کارت دستگاه.
- دریافت و نمایش پیامک‌های پاسخ و گزارش‌های دستگاه.
- مدیریت شماره تلفن‌های مجاز و مدیران دستگاه.
- نمایش وضعیت دزدگیر، ورودی‌ها، خروجی‌ها و هشدارها.
- ذخیره سوابق فرمان‌ها، پاسخ‌ها و رویدادهای امنیتی.

- امکان استفاده از اپلیکیشن در موبایل، تبلت و رایانه.
- فراهم کردن زیرساخت توسعه قابلیت‌های جدید در آینده.

۳. امکانات صفحه اصلی

پس از ورود کاربر، صفحه اصلی باید اطلاعات زیر را نمایش دهد:

- نام و شناسه دستگاه.
- شماره سیم کارت نصب شده روی دستگاه.
- وضعیت دزدگیر: فعال، غیرفعال یا نیمه فعال.
- وضعیت حالت بی صدا.
- وضعیت برق اصلی دستگاه.
- وضعیت باتری پشتیبان، در صورت پشتیبانی سخت افزار.
- وضعیت ورودی‌ها و زون‌های دزدگیر.
- وضعیت خروجی‌های قابل کنترل.
- آخرین هشدارها و رویدادهای ثبت شده.
- زمان آخرین ارتباط موفق با دستگاه.

وضعیت‌هایی که مستقیماً از دستگاه قابل دریافت نیستند، نباید به عنوان وضعیت قطعی نمایش داده شوند. برای مثال، ارسال موفق پیامک به معنی اجرای قطعی فرمان توسط دزدگیر نیست.

۴. کنترل دزدگیر

در صفحه کنترل دستگاه، فرمان‌های زیر باید در دسترس باشند:

فرمان	عملکرد
ARM	فعال کردن کامل دزدگیر
DISARM	غیرفعال کردن دزدگیر
PARTSET	فعال کردن حالت نیمه فعال
SILENT	فعال یا غیرفعال کردن حالت بی صدا، مطابق پروتکل دستگاه
Door open	درب باز کن
OUT1 ON/OFF	روشن یا خاموش کردن خروجی اول دائم/لحظه ای
OUT2 ON/OFF	روشن یا خاموش کردن خروجی دوم دائم/لحظه ای

OUT3 ON/OFF روشن یا خاموش کردن خروجی سوم دائم / لحظه ای

OUT4 ON/OFF روشن یا خاموش کردن خروجی چهارم دائم / لحظه ای

فرمان‌ها باید مطابق پروتکل واقعی دستگاه تولید شوند. نام‌های بالا نام عملکردها هستند و لزوماً متن پیامک ارسالی نیستند.

الزامات اجرای فرمان

۱. کاربر فرمان موردنظر را انتخاب کند.
۲. سامانه پیامک متناظر با فرمان را به شماره سیم‌کارت دستگاه ارسال کند.
۳. وضعیت فرمان در رابط کاربری به صورت «در انتظار پاسخ» نمایش داده شود.
۴. پس از دریافت پاسخ معتبر از دستگاه، نتیجه واقعی فرمان ثبت و نمایش داده شود.
۵. اگر پاسخ در بازه زمانی تعیین شده دریافت نشد، وضعیت «بدون پاسخ» یا «نامشخص» نمایش داده شود.
۶. برای جلوگیری از اجرای ناخواسته عملیات، سامانه نباید پیامک‌های فرمان را بدون بررسی شرایط، به صورت خودکار و نامحدود تکرار کند.

۵. مدیریت دستگاه‌ها

سامانه باید امکان ثبت و مدیریت چند دستگاه را داشته باشد.

اطلاعات هر دستگاه شامل موارد زیر باشد:

- نام دلخواه دستگاه.
- شناسه یکتا.
- شماره سیم‌کارت دستگاه.
- مدل و نسخه سخت‌افزار.
- نسخه نرم‌افزار یا Firmware، در صورت دسترسی.
- توضیحات و محل نصب.
- کاربران مجاز به کنترل دستگاه.
- زمان آخرین پاسخ معتبر دستگاه.

هر کاربر فقط باید به دستگاه‌هایی دسترسی داشته باشد که مالک آن‌هاست یا مجوز مدیریت آن‌ها را دارد.

۶. مدیریت شماره‌های تلفن

در پنل مدیریت هر دستگاه باید امکان ثبت، ویرایش و حذف شماره‌های تلفن وجود داشته باشد.

قابلیت‌های موردنیاز:

- ثبت شماره تلفن با کد کشور.
- نام‌گذاری هر شماره.
- تعیین سطح دسترسی هر شماره.
- تعیین مجوز دریافت هشدارها و گزارش‌ها.
- نمایش وضعیت فعال یا غیرفعال بودن شماره.
- جلوگیری از ثبت شماره‌های تکراری برای یک دستگاه.
- ثبت سوابق تغییرات شماره‌ها.

در صورت پشتیبانی Firmware دستگاه، حداکثر ۳۰ شماره تلفن ذخیره‌شده باید بتوانند به‌عنوان مدیر یا شماره مجاز تعریف شوند. محدودیت‌های واقعی دستگاه باید در طراحی نهایی لحاظ شوند.

۷. دریافت هشدارها و گزارش‌ها

وب‌اپلیکیشن باید بتواند گزارش‌های دریافتی از دستگاه را دسته‌بندی و نمایش دهد.

انواع رویدادهای موردنیاز:

- فعال و غیرفعال شدن دزدگیر.
- فعال شدن حالت نیمه‌فعال.
- وقوع آژیر در هر زون.
- باز و بسته شدن ورودی‌های تعریف‌شده.
- قطع و وصل برق اصلی.
- وضعیت باتری پشتیبان، در صورت پشتیبانی.
- روشن و خاموش شدن خروجی‌ها.
- روشن یا خاموش شدن پمپ یا تجهیزات متصل، در صورت تعریف.
- هشدارهای مربوط به درب، مخزن یا سایر ورودی‌های سفارشی.
- خطاهای ارتباطی و پاسخ‌های نامعتبر.

برای هر رویداد باید تاریخ و ساعت، دستگاه مربوطه، نوع رویداد و متن پیامک ذخیره شود.

۸. تاریخچه و گزارش گیری

یک بخش مجزا برای مشاهده سوابق در نظر گرفته شود.

امکانات این بخش:

- نمایش تاریخچه فرمان های ارسال شده.
- نمایش پیامک های دریافتی.
- تفکیک فرمان های موفق، ناموفق و بدون پاسخ.
- فیلتر بر اساس دستگاه، نوع رویداد و بازه زمانی.
- جست و جو در گزارش ها.
- امکان خروجی گرفتن از گزارش ها در قالب CSV یا Excel.
- ثبت تاریخ و ساعت با منطقه زمانی مشخص.

۹. معماری ارتباط پیامکی

وب اپلیکیشن مستقیماً به سیم کارت نصب شده داخل دزدگیر متصل است؛

معماری پیشنهادی:

۱. کاربر در وب اپلیکیشن فرمانی صادر می کند.
۲. Backend. هویت کاربر و مجوز دسترسی او را بررسی می کند.
۳. برنامه فرمان را از طریق متن پیامک به سیم کارت دزدگیر ارسال می کند
۴. دستگاه پیامک را دریافت و فرمان را اجرا می کند.
۵. دستگاه پیامک پاسخ یا گزارش را به شماره تعیین شده ارسال می کند.
۶. وب اپلیکیشن پیامک دریافتی را تحلیل و تغییرات گرافیکی جهت نمایش به کاربر را اعمال می کند.
۷. چون پیامک دریافت می شود میتوان آخرین تغییرات را در بررسی و در برنامه اعمال کرد لذا تغییرات با هر بازو بسته شدن برنامه چک شده و اعمال شود.

۱۰. امنیت سامانه

از آنجا که سامانه امکان کنترل یک سیستم امنیتی فیزیکی را دارد، امنیت باید از الزامات اصلی پروژه باشد.

موارد الزامی:

- ورود امن با نام کاربری و رمز عبور.
- کنترل دسترسی کاربران به دستگاه‌ها.
- نگهداری امن کلیدها و اطلاعات سرویس پیامکی.
- جلوگیری از تزریق فرمان و ارسال پیامک غیرمجاز.
- عدم نمایش اطلاعات محرمانه در گزارش‌های عمومی.

۱۱. طراحی رابط کاربری

رابط کاربری باید:

- کاملاً فارسی و راست‌چین (RTL) باشد.
- طراحی واکنش‌گرا داشته باشد.
- روی موبایل اندروید و iOS، تبلت و دسکتاپ به درستی نمایش داده شود.
- دکمه‌های فرمان واضح و قابل تشخیص داشته باشد.
- برای فرمان‌های حساس، تأییدیه نمایش دهد.
- وضعیت انتظار، موفقیت، خطا و عدم دریافت پاسخ را تفکیک کند.
- از رنگ‌ها و علائم بصری برای نمایش وضعیت‌ها استفاده کند.
- در صورت امکان، به شکل PWA قابل نصب روی صفحه اصلی موبایل باشد.

۱۲. فناوری‌های پیشنهادی

انتخاب فناوری نهایی بر عهده برنامه‌نویس است، اما معماری باید توسعه‌پذیر و قابل نگهداری باشد.

اجزای پیشنهادی:

- Frontend: React یا Vue.js
- Backend: Node.js، Laravel یا فناوری مشابه.
- Database: PostgreSQL یا MySQL

- ارتباط پیامکی: پنل SMS ارسال و دریافت پیامک.

۱۳. الزامات عملکردی و پایداری

- ارسال و دریافت پیامک باید غیرهمزمان انجام شود تا رابط کاربری متوقف نشود.
- در صورت قطعی سرویس پیامکی، خطا به کاربر اعلام شود.
- از ثبت چندباره یک رویداد به علت دریافت پیامک تکراری جلوگیری شود.
- پیامک‌های دیررس با زمان دریافت و زمان گزارش شده، در صورت وجود، ثبت شوند.
- محدودیت ارسال پیامک برای جلوگیری از هزینه ناخواسته وجود داشته باشد.
- سامانه باید امکان پشتیبان‌گیری و بازیابی اطلاعات را داشته باشد.

۱۴. معیارهای تحویل پروژه

پروژه زمانی قابل قبول است که:

۱. کاربر بتواند وارد سامانه شود و دستگاه خود را ثبت کند.
۲. فرمان‌های اصلی دزدگیر را از طریق رابط کاربری ارسال کند.
۳. نتیجه ارسال و پاسخ واقعی دستگاه را به صورت مجزا مشاهده کند.
۴. پیامک‌های هشدار و رویدادها دریافت و ذخیره شوند.
۵. شماره‌های مجاز و سطح دسترسی آن‌ها مدیریت شوند.
۶. تاریخچه فرمان‌ها و هشدارها قابل جست‌وجو باشد.
۷. سامانه روی موبایل و رایانه به درستی کار کند.
۸. سورس‌کد، ساختار پایگاه داده و اطلاعات لازم برای استقرار به کارفرما تحویل داده شود.

۱۵. مواردی که پیش از شروع توسعه باید مشخص شوند

- متن دقیق پیامک هر فرمان.
- متن دقیق پاسخ‌های دستگاه.
- شماره سیم‌کارت دستگاه و نحوه تعریف شماره مدیر.

- روش دریافت SMS های ورودی.
- امکان یا عدم امکان تغییر Firmware دزدگیر.
- تعداد دستگاه های مورد نیاز در نسخه اول.
- تعداد کاربران و سطح دسترسی آنها.
- سرویس پیامکی مورد استفاده و هزینه هر پیامک.
- نیاز به اعلان از طریق پیامک، اعلان مرورگر یا هر دو.

جمع بندی

هدف، ساخت یک پنل مدیریتی تحت وب برای کنترل دزدگیر سیم کارتی با استفاده از SMS است؛ به گونه ای که کاربر بتواند با هر وسیله ارتباطی (گوشی اندروید /IOS/ تبلت یا پنل SMS) فرمان صادر کند، پاسخ دستگاه را دریافت کند و سوابق هشدارها را ببیند.

توسعه باید به صورت ماژولار انجام شود تا در آینده بتوان قابلیت هایی مانند مدیریت چند دستگاه، تعریف کاربران متعدد، اعلان های پیشرفته و پشتیبانی از مدل های جدید دزدگیر را اضافه کرد.

خروجی مورد انتظار از برنامه نویسی: وب اپلیکیشن عملیاتی، اتصال کامل به سرویس ارسال و دریافت SMS، مستندات فنی و سورس کد قابل توسعه.